UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/955,165 | 09/19/2001 | Christoph Cornelius Michael | CIG-105 | 8323 |

28970 7590 10/14/2005

PILLSBURY WINTHROP SHAW PITTMAN LLP
1650 TYSONS BOULEVARD
MCLEAN, VA 22102

| EXAMINER | |
|---|---|
| HIRL, JOSEPH P | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2129 | |

DATE MAILED: 10/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/955,165 | MICHAEL, CHRISTOPH CORNELIUS | |
| | Examiner | Art Unit | |
| | Joseph P. Hirl | 2129 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *03 August 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 September 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

1. This Office Action is in response to an AMENDMENT entered August 3, 2005 for the patent application 09/955,165 filed on September 19, 2001.

2. The First Office Action of February 3, 2005 is fully incorporated into this Final Office Action by reference.

### *Status of Claims*

3. Claims 2-20 are new. Claims 1-20 are pending.

### *Claim Rejections - 35 USC § 112*

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 2, 4, 16 and 18 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The terms discretely, novel, malicious, damaging and elevating, respectively from the subject claims are relative and render claims 2, 4, 16, and 18 indefinite.

***Claim Rejections - 35 USC § 102***

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Hines et al. (U.S. Pub. 2003/0121027, referred to as **Hines**).

**Claim 1**

Hines anticipates generating a normal execution trace for the software program (**Hines**, p 0483); applying a learning algorithm to the normal execution trace to build a finite automaton (**Hines**, p 0489; Examiner's Note (EN): p 13. below applies; a debugger is a learning algorithm used to build a finite automaton ... an operating program); applying an examination algorithm to find the finite automaton to identify undesirable transition states in the finite automaton and to create a labeled finite automaton (**Hines**, p 0489; 0481, l 5-11; EN: the debugger is also an examination algorithm that identifies undesirable transition states to create a working (labeled) finite automaton); and applying the labeled finite automaton to an execution trace with the executing software program (**Hines**, p 0489; 0481, l 5-11; 0643-0652).

**Claim 2**

Hines anticipates application of the learning algorithm occurs during a first learning, phase and application of the examination algorithm occurs during a second, examination phase and the learning phase occurs before and discretely from the examination phase (**Hines**, p 0002; EN: p 13. applies; debugging involves the detection, location and correction of logical or syntactical errors or malfunctions in a program/hardware; a debugger involves an algorithm; detecting and locating an error is a learning process; correction of the error is separate from and follows the detecting and locating process; correcting is a step process or algorithm).

**Claim 3**

Hines anticipates the labeled finite automaton identifies undesirable behavior (**Hines**, p 0002; EN: p 13. applies; such is the reason for using a debugger).

**Claim 4**

Hines anticipates application of the labeled finite automaton to the execution trace is performed to identify undesirable behavior in a novel execution trace (**Hines**, p 0002; 0476, 0477; Fig. 39; EN: p 13. applies; a debugger is a finite state automaton; an undesirable behavior is illustrated in Fig. 39 that involves messaging from the future to the past.

**Claim 5**

Hines anticipates the undesirable behavior comprises the undesirable transition (**Hines**, p 0002; Fig. 39; EN: see discussion above).

**Claim 6**

Hines anticipates the finite automaton comprises a tuple (**Hines**, p 0160 – 0163).

**Claim 7**

Hines anticipates wherein the tuple comprises a set of possible states, a set of symbols comprising the input alphabet, a mapping function, a start state, and a set of final states (**Hines**, p 0159 – 0168).

**Claim 8**

Hines anticipates the tuple comprises a set of states interconnected by labeled transitions (**Hines**, p 0159 – 0168; Fig. 4B).

**Claim 9**

Hines anticipates finite automaton comprises a prefix tree (**Hines**, Fig. 30; EN: a space time graph is equivalent to a prefix tree).

**Claim 10**

Hines anticipates the prefix tree comprises a plurality of nodes (**Hines**, Fig. 30; EN: see above reference and discussion).

**Claim 11**

Hines anticipates the plurality of the nodes of the prefix tree correspond to states of the finite automaton (**Hines**, Fig. 30; EN: p 13 applies; it is finite and moves through the identified states).

**Claim 12**

Hines anticipates one of the plurality of nodes comprises a root node, with the root node serving as a start state (**Hines**, Fig. 37).

**Claim 13**

Hines anticipates a remainder of the plurality of nodes comprise accepting states (**Hines**, Fig. 37; EN: p 13 applies; nodes remain and will accept states).

**Claim 14**

Hines anticipates the learning algorithm selectively merges nodes in the finite automaton (**Hines**, p 0304).

**Claim 15**

Hines anticipates the learning algorithm comprises a state merging algorithm. (**Hines**, p 0304; EN: p 13. applies; state merging is equivalent to merging of schedules).

**Claim 16**

Hines anticipates flagging the execution trace associated with the executing software program as malicious if the execution trace associated with the executing software program is rejected by the finite automaton (**Hines**, p 0516).

**Claim 17**

Hines anticipates wherein the execution trace associated with the executing software program is rejected if it does not end in an accepting state (**Hines**, p 0516; EN: p 13. applies; such is when a white process receives a red message).

**Claim 18**

Hines anticipates the undesirable behavior comprises at least one of providing an undesired method of entry into the system to unauthorized users, damaging system resources, and elevating user privileges (**Hines**, p 0316-0320; p 0003; p 0128; EN: p 13. applies; undesired method would be in appropriate actions implemented when the

monitor mode is executed; damaging resources occur when implementation time is excessive; evaluating user privileges occurs when tokens are assigned).

**Claim 19**

Hines anticipates the finite automaton is built using empirical data (**Hines**, p 0249; EN: p 13. applies; building of subsumption protocol uses empirical data).

**Claim 20**

Hines anticipates monitoring processes at a system level (**Hines**, Abstract).

***Response to Arguments***

8. The rejection of claim 1 under 35 USC 101 is withdrawn.

9. Applicant's arguments filed on August 3, 2005 related to the subject claims have been fully considered but are not persuasive.

In reference to Applicant's argument:

Turning to the rejection under 35 U.S.C. § 102(e) as being anticipated by Hines et al., Applicants respectfully disagree with the Examiner's characterization of Hines as teaching the requisite "method for detecting anomalous behavior." The portions of Hines cited by the Examiner do not relate to detecting anomalous behavior as is recited in claim 1. Specifically, Applicants assert that there is no teaching in Hines at least of identifying "undesirable transition states in the finite automaton," nor creating "a labeled finite automaton" as recited in claim 1. Hines discusses only debugging software, and paragraph 0481, cited in the Office Action, merely discusses "consistent cuts," which appear to have nothing to do with identifying undesirable transition states as recited in claim 1 and the Office Action provides no explanation as to how these consistent cuts taught by Hines correspond to specific recitations of claim 1.

Examiner's response:

Para 13 applies. The Examiner has full latitude to interpret each claim in the broadest reasonable sense. Limitations appearing in the specification but not recited in the claim are not read into the claim. The claims and only the claims form the metes and bounds of the invention. A finite automaton is a program that runs a machine such

as a computer. Figure 39 would be part of a labeled finite automaton. Undesirable transition states in such a program are states where the computer would venture in an operation that is not defined or violate an unacceptable rule. Hines identifies and defines cuts to be either consistent or inconsistent (0481 and 0482). Inconsistent cuts identify a message process from the future to the past ... unacceptable transition state.

In reference to Applicant's argument:

While the Examiner is permitted to give claims their broadest reasonable interpretation, this does not permit the Examiner to essentially ignore specific recitations as the present rejection seemingly attempts to do. The present invention relates, in one aspect, generally to anomaly detection to address the problem of detecting new or novel system attacks (see specification p. 2), while Hines generally relates to locating a predetermined sequence of events or predetermined behavior and acting accordingly (see Hines abstract). Hines does not discuss application of a learning algorithm and an examination algorithm to detect novel behavior, which by definition, would not be a "predetermined sequence of events" as is taught in Hines.

Examiner's response:

Para 13 applies. The Examiner has full latitude to interpret each claim in the broadest reasonable sense. Limitations appearing in the specification but not recited in the claim are not read into the claim. The claims and only the claims form the metes and bounds of the invention. Use of a debugger represents a learning process or algorithm, related to anomaly detection to identify the reasons why a software system or part thereof fails to function properly ... anomaly detection. The evaluation follows the debugger, facilitating analysis of message transition ... Fig. 39.

In reference to Applicant's argument:

Further, although the Examiner has pointed to various portions of Hines that allegedly teach recitations of claim 1 (without any explanation of how the different terminology and methodology of Hines allegedly teach the claimed recitations), Applicants assert that these cited portions have practically no relation to

the recitations of claim 1. For example, paragraph 0481 of Hines does not discuss anything having to do with the claimed identification of "undesirable transition states in the finite automaton." A "broad interpretation" of claim language does not allow the Examiner to redefine the teachings of a cited reference in a manner not contemplated by that reference. Other than the fact that Hines recites the term "automata" at some points in the disclosure, Applicant does not agree that Hines teaches many, if any, of the recitations of claim 1. If the Examiner chooses to apply Hines in any future office action, Applicant would appreciate an explanation of the application of Hines as Applicant currently believes that the present rejection fails to meet the prima facie standard for rejection under 35 U.S.C. §102(e).

Examiner's response:

Para 13 applies. The Examiner has full latitude to interpret each claim in the broadest reasonable sense. Limitations appearing in the specification but not recited in the claim are not read into the claim. The claims and only the claims form the metes and bounds of the invention. State Based debugging further identifies Hines' state of the system or automaton approach.

Regarding the Applicant's statement on the prima facie standard, the following applies from CFR 37 1.56(b)(2)(ii):

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden of proof standard, giving each term in the claim it broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

In the First Office Action dated February 3, 2005, the claim and each of the items in the claim was referenced to appropriate sections of related art given in U.S. Pub 2003/0121027 as further discussed above.

***Examination Considerations***

10. The claims and only the claims form the metes and bounds of the invention. "Office personnel are to give the claims their broadest reasonable interpretation in light

of the supporting disclosure. *In re Morris,* 127 F.3d 1048, 1054-55, 44USPQ2d 1023, 1027-28 (Fed. Cir. 1997). Limitations appearing in the specification but not recited in the claim are not read into the claim. *In re Prater*, 415 F.2d, 1393, 1404-05, 162 USPQ 541, 550-551 (CCPA 1969)" (MPEP p 2100-8, c 2, l 45-48; p 2100-9, c 1, l 1-4). The Examiner has full latitude to interpret each claim in the broadest reasonable sense. Examiner will reference prior art using terminology familiar to one of ordinary skill in the art. Such an approach is broad in concept and can be either explicit or implicit in meaning.

11. Examiner's Notes are provided with the cited references to prior art to assist the applicant to better understand the nature of the prior art, application of such prior art and, as appropriate, to further indicate other prior art that maybe applied in other office actions. Such comments are entirely consistent with the intent and spirit of compact prosecution. However, and unless otherwise stated, the Examiner's Notes are not prior art but a link to prior art that one of ordinary skill in the art would find inherently appropriate.

12. Unless otherwise annotated, Examiner's statements are to be interpreted in reference to that of one of ordinary skill in the art. Statements made in reference to the condition of the disclosure constitute, on the face of it, the basis and such would be obvious to one of ordinary skill in the art, establishing thereby an inherent prima facie statement.

13. Examiner's Opinion: paras 10-12 apply. The Examiner has full latitude to interpret each claim in the broadest reasonable sense.

***Conclusion***

14. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

15. Claims 1-20 are rejected.

***Correspondence Information***

16. Any inquiry concerning this information or related to the subject disclosure should be directed to the Examiner, Joseph P. Hirl, whose telephone number is (571) 272-3685. The Examiner can be reached on Monday – Thursday from 6:00 a.m. to 4:30 p.m.

If attempts to reach the Examiner by telephone are unsuccessful, the

Examiner's supervisor, David R. Vincent can be reached at (571) 272-3080.

Any response to this office action should be mailed to:

Commissioner of Patents and Trademarks,

Washington, D. C. 20231;

Hand delivered to:

Receptionist,

Customer Service Window,

Randolph Building,

401 Dulany Street,

Alexandria, Virginia 22313,

(located on the first floor of the south side of the Randolph Building);

or faxed to:

(571) 273-8300 (for formal communications intended for entry.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have any questions on access to Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll free).

Joseph P. Hirl
Primary Examiner
October 12, 2005